Discrete Mathematics 25 (1979) 269–273

MAXIMAL SETS OF PERMUTATIONS CONSTRUCTED FROM PROJECTIVE PLANES

Peter LORIMER
Universität Kaiserslautern, Mathematik, Postfach 3049, 6750 Kaiserslautern, Germany

Received 7 March 1978
Revised 11 September 1978

On the set of n^2+n+1 points of a projective plane, a set of n^2+n+1 permutations is constructed with the property that any two are a Hamming distance $2n+1$ apart. Another set is constructed in which every pair are a Hamming distance not greater than $2n+1$ apart. Both sets are maximal with respect to the stated property.

An equidistant permutation array, or EPA, is a set of permutations on a finite set, each pair of which have the same image at the same number of points; a maximal EPA is one which cannot be extended without spoiling this property. The first construction produces, from a projective plane of order n, a maximal EPA of n^2+n+1 permutations on the n^2+n+1 points of the plane, each pair of which have the same image at n^2-n points. In the notation of [1] this is a maximal $A(n^2+n+1,\ n^2-n;\ n^2+n+1)$.

The second construction, also from a projective plane of order n, is of a maximal $A(n^2+n+1, \geq(n^2-n); m)$ where the exact value of m will be described later. This permutation array contains m permutations on the n^2+n+1 points of the plane, each pair of which have the same image at not less than n^2-n points.

If two permutations on a set with σ members have the same image at λ points they are said to be a Hamming distance $\sigma-\lambda$ apart. Distance here will always mean Hamming distance. If x has the same image under two permutations it will be said that they coincide at x.

1. The maximal $A(n^2+n+1, n^2-n; n^2+n+1)$

Let $\mathcal{P}$ be the set of points in a projective plane π of order n, and for each line L of π, let p_L be a permutation of $\mathcal{P}$ which moves every point of L and fixes every point of the plane not on L. Let $\mathcal{M}$ be a set of permutations like this, one for each line of the plane.

For example: let π be the projective plane of order 2 having points $1, 2, 3, 4, 5, 6, 7$ and lines $\{1, 2, 3\}$, $\{3, 4, 5\}$, $\{5, 6, 1\}$, $\{1, 7, 4\}$, $\{3, 7, 6\}$, $\{2, 7, 5\}$, $\{2, 4, 6\}$. The 3-cycle (123) moves each of the points on the first line and fixes each of the other four points of the plane.

$$\mathcal{M}=\{(123), (345), (561), (174), (376), (275), (246)\}$$

1	2	3	4	5	6	7
2	3	1	4	5	6	7
1	2	4	5	3	6	7
5	2	3	4	6	1	7
7	2	3	1	5	6	4
1	2	7	4	5	3	6
1	7	3	4	2	6	5
1	4	3	6	5	2	7

Fig. 1.

is a suitable set of permutations; this set can be used to construct the array in Fig. 1, each permutation contributing one line.

It can be easily seen that each pair of rows have exactly two common entries, so that this is an example of an $A(7, 2; 7)$.

Theorem 1. *$\mathcal{M}$ is a maximal $A(n^2+n+1,\ n^2-n;\ n^2+n+1)$.*

Proof. Obviously any two permutations of $\mathcal{M}$ coincide on the n^2-n points not lying on the two lines used to define them, and they don't coincide anywhere else.

Let f be a permutation which it is proposed to add to $\mathcal{M}$ with the intention of forming a bigger set with the same equidistant property that $\mathcal{M}$ has. Suppose that f fixes α points of $\mathcal{M}$ and moves $n^2+n+1-\alpha$.

If f fixes a point x, it coincides at x with the permutation p_L if and only if x does not lie on the line L. As there are n^2 lines on which x does not lie, f coincides at x with n^2 permutations of $\mathcal{M}$.

If f moves y, then f coincides at y with at most one permutation of $\mathcal{M}$, the one p_L that moves points on the line L joining y and $f(y)$.

Hence the total number of coincidences between f and members of $\mathcal{M}$ cannot be greater than

$$n^2\alpha+(n^2+n+1-\alpha).$$

On the other hand f coincides with each of the n^2+n+1 permutations of $\mathcal{M}$ at exactly n^2-n points. Hence

$$(n^2+n+1)(n^2-n)\leq n^2\alpha+(n^2+n+1-\alpha),$$

an inequality which leads to

$$\alpha\geq n^2-1+\frac{n^2-2n}{n^2-1}$$

and on to

$$\alpha>n^2-1$$

except when $n=2$ and $\alpha=3$.

Consider a line L of π. The permutation p_L coincides with f at n^2-n points: hence at most n^2-n of the α points fixed by f do not lie on L and the number of points of L fixed by f is greater than

$$(n^2-1)-(n^2-n)=n-1$$

except possibly when $n=2$ and $\alpha=3$. However, if f moves a point x, it also moves $f(x)$ so that it fixes at most $n-1$ points on at least one line. This contradiction establishes that $\mathcal{M}$ is maximal except in the case that $n=2$ and $\alpha=3$.

Suppose that $n=2$ and $\alpha=3$. If the three fixed points of f form a triangle, let L be the line of the plane not passing through any of the fixed points; then the three fixed points will also be fixed points of p_L and f coincides with p_L in at least three places, contrary to assumption. If the three fixed points lie on a line K, then f does not coincide with p_K at any of the points of K; hence it does coincide with p_K at two points not on K, a contradiction as p_K fixes every point not on K.

This proves Theorem 1.

2. The maximal $A(n^2+n+1,\geq(n^2-n);m)$

Let $\mathcal{P}$ be the set of points of a projective plane π of order n, let $\mathcal{M}_1$ be the set of all permutations of $\mathcal{P}$ which fix more than n^2 points and let $\mathcal{M}_2$ be the set of all permutations of $\mathcal{P}$ which fix at least the n^2 points not lying on some line of the plane. Put $\mathcal{M}=\mathcal{M}_1\cup\mathcal{M}_2$.

Theorem 2. *$\mathcal{M}$ is a maximal $A(n^2+n+1,\geq(n^2-n);m)$ where*

$$m=1+\sum_{i=1}^{n-1}\binom{n^2+n+1}{n^2+n+1-i}D_{i+1}+(n^2+n+1)D_{n+1}$$

where D_i is the number of derangements of i symbols or the number of permutations on i symbols which have no fixed points.

Proof. The first part of the proof shows that $\mathcal{M}$ is indeed an $A(n^2+n+1,\geq(n^2-n),m)$.

First, a permutation from $\mathcal{M}_1$ fixes more than n^2 points and one from $\mathcal{M}_2$ fixes more than n^2-1; thus each coincides with the identity in at least n^2-n places.

A permutation from $\mathcal{M}_1$ moves at most n points and one from $\mathcal{M}_2$ moves at most $n+1$.

A permutation from $\mathcal{M}_1$ and any permutation from $\mathcal{M}$ thus fix in common at least

$$n^2+n+1-n-(n+1)=n^2-n$$

points.

If two non-identity permutations come from $\mathcal{M}_2$ they fix at least n^2 points if both move only points on the same line; if they move points on two lines they fix at least the n^2-n points not on the union of the lines.

This proves that $\mathcal{M}$ is an $A(n^2+n+1, \geq (n^2-n); m)$.

The proof that $\mathcal{M}$ is maximal is similar in principle to the corresponding proof in the first section.

Let f be a permutation of $\mathcal{P}$ which it is proposed to join to $\mathcal{M}$ without altering its distance property. Suppose that f fixes α points and moves $n^2+n+1-\alpha$.

If f fixes a point x, it fixes x in common with each of the permutations of $\mathcal{M}_2$ which move points on one of the n^2 lines not passing through $\mathcal{P}$. The number of permutations like this, excluding the identity, is

$$n^2((n+1)!-1)$$

If f moves a point x it has the same effect on x as do $n!$ of the $(n+1)!$ permutations of $\mathcal{M}_2$ which move points on the line joining x and $f(x)$.

Hence the number of times that f has the same effect as a permutation of $\mathcal{M}_2-\{1\}$ is

$$n^2((n+1)!-1)\alpha+n!(n^2+n+1-\alpha)$$

The set $\mathcal{M}_2-\{1\}$ has $(n^2+n+1)((n+1)!-1)$ members so that the assumption in the theorem implies that

$$(n^2+n+1)((n+1)!-1)(n^2-n) \leq$$
$$\leq n^2((n+1)!-1)\alpha+n!(n^2+n+1-\alpha).$$

Now

$$(n^2+n+1)(n^2-n) \leq (n^2+n+1)n!$$

and

$$n^2\alpha \geq 0.$$

Hence the inequality in the last paragraph leads to

$$(n^2+n+1)((n^2-n)(n+1)!-n!) \leq$$
$$\leq n^2(n+1)!\alpha+(n^2+n+1-\alpha)n!$$

to

$$(n^2+n+1)((n^2-n)(n+1)-1) \leq$$
$$\leq (n^2(n+1)\alpha+(n^2+n+1-\alpha))$$

and to

$$\alpha \geq \frac{n^5+n^4-3n^2-3n-2}{n^3+n^2-1}$$
$$= n^2-1+\frac{n^3-n^2-3n-3}{n^3+n^2-1}.$$

Hence

$$\alpha \geq n^2$$

except possibly when $n=2$ and $\alpha=3$.

On the other hand, $\mathcal{M}$ contains every permutation of $\mathcal{P}$ which fixes more than n^2 points so that

$$\alpha \leq n^2.$$

Suppose $\alpha = n^2$ and f moves $n+1$ points. As f is not a member of $\mathcal{M}_2$ these $n+1$ points are not collinear. Let L be a line passing through two of them and let x be a point of L which is fixed by f. As there are $n+1$ lines through x and one of them contains 2 points moved by f, one of them, say K, contains only points fixed by f. Let g be one of the permutations of $\mathcal{M}_2$ which moves every point of K and fixes every point not on K. The permutation f coincides with g in at least n^2-n points, none of which can lie on K. Hence f fixes a total of at least $(n^2-n)+(n+1)=n^2+1$ points, a contradiction.

This proves that $\mathcal{M}$ is maximal except possibly when $n=2$ and $\alpha=3$.
In this last case, let L be a line through 2 of the points fixed by f and let g be one of the permutations of $\mathcal{M}_2$ which fixes none of the points of L and fixes all of the points not on L. This permutation cannot coincide with f at any point of L so it must coincide with it in at least two points not on L. Thus f fixes these two points to give a total of at least 4 fixed points, a contradiction.

This proves Theorem 2.

Acknowledgement

I am indebted to Mikhail Deza for conversations on the topic discussed here.

Reference

[1] M. Deza and S.A. Vanstone, Bounds for permutation arrays (to appear).